UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,108	02/08/2002	Joseph J. Pantuso	NAI1P095/02.014.01	2543

28875 7590 10/04/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 10/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/072,108	PANTUSO, JOSEPH J.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/19/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on 6/19/2002 is being considered by the examiner. An initialed copy of IDS is attached to this office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1 – 20 rejected under 35 U.S.C. 102(b) as being anticipated by Conklin et al. (U.S. Patent Number 5,796,942).

3. Regarding Claim 1, Conklin teaches establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55); and

transmitting a response to the firewalls of the computers utilizing the network (Summary and Column 4 lines 9 – 29);

wherein the firewalls are adapted for preventing the intrusion activity utilizing the response (Summary and Column 4 lines 9 – 29).

4. Regarding Claim 8, Conklin teaches logic for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

logic for collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55); and

logic for transmitting a response to the firewalls of the computers utilizing the network (Summary and Column 4 lines 9 – 29);

wherein the firewalls are adapted for preventing the intrusion activity utilizing the response (Summary and Column 4 lines 9 – 29).

5. Regarding Claim 9, Conklin teaches computer code for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

computer code for collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55); and

computer code for transmitting a response to the firewalls of the computers utilizing the network (Summary and Column 4 lines 9 – 29);

wherein the firewalls are adapted for preventing the intrusion activity utilizing the response (Summary and Column 4 lines 9 – 29).

6. Regarding Claim 10, Conklin teaches establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55);

analyzing the information to ascertain intrusion activity(Summary and Column 4 line 46 – Column 5 line 22);

identifying a source of the ascertained intrusion activity (Summary and Column 5 lines 9 – 29); and

notifying the source of the ascertained intrusion activity (Summary and Column 5 lines 15 – 61).

7. Regarding Claim 19, Conklin teaches logic for establishing network communications with a plurality of computers with firewalls over a network, wherein the

firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

logic for collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55);

logic for analyzing the information to ascertain intrusion activity (Summary and Column 4 line 46 – Column 5 line 22);

logic for identifying a source of the ascertained intrusion activity (Summary and Column 5 lines 9 – 29); and

logic for notifying the source of the ascertained intrusion activity (Summary and Column 5 lines 15 – 61).

8. Regarding Claim 20, Conklin teaches computer code for establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

computer code for collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55);

computer code for analyzing the information to ascertain intrusion activity (Summary and Column 4 line 46 – Column 5 line 22);

computer code for identifying a source of the ascertained intrusion activity (Summary and Column 5 lines 9 – 29); and

computer code for notifying the source of the ascertained intrusion activity (Summary and Column 5 lines 15 – 61).

9. Regarding Claim 21, Conklin teaches collecting information relating to intrusion activity utilizing a firewall associated with a computer (Summary and Column 3 lines 37 – 43);

transmitting the information from the firewall associated with the computer to a central server utilizing the network (Summary and Column 4 lines 9 – 29);

receiving a response from the central server utilizing the network (Summary and Column 4 lines 9 – 29);

wherein the firewall is adapted for preventing the intrusion activity utilizing the response (Summary and Column 4 lines 9 – 29).

10. Regarding Claim 22, Conklin teaches establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity (Summary and Column 3 lines 37 – 43);

collecting the information from the firewalls of the computers utilizing the network (Summary and Column 3 lines 37 – 55);

heuristically analyzing the information to ascertain intrusion activity (Summary and Column 4 line 46 – Column 5 line 22);

generating rules for preventing the intrusion activity utilizing the firewalls based on the heuristic analysis (Summary and Column 4 line 45 – Column 5 line 22);

transmitting the rules to the firewalls of the computers utilizing the network, wherein the firewalls are adapted for preventing the intrusion activity utilizing the rules (Summary and Column 4 lines 9 – 29);

identifying an Internet Protocol (IP) address associated with at least one source of the intrusion activity (Summary and Column 5 lines 26 – 45);

looking up an electronic-mail address based on the IP address (Summary and Column 5 line 26 – Column 6 line 12);

generating a summary of the information relating to the intrusion activity associated with the source (Summary and Column 6 lines 20 – 27);

transmitting the summary to the electronic-mail address in the form of electronic-mail (Summary and Column 7 line 17 – Column 8 line 13);

determining whether a response to the electronic-mail is received; and if it is determined that the response to the electronic-mail is not received, reporting the source of the intrusion activity to a central intrusion activity watch service, wherein the central intrusion activity watch service notifies the public of the source of the intrusion activity via a web interface (Summary and Column 8 lines 1 – 24).

11. Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches heuristically analyzing the information to ascertain intrusion activity (Summary and Column 4 line 46 – Column 5 line 22).

12. Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches generating rules for preventing the intrusion activity utilizing the firewalls (Summary and Column 4 line 45 – Column 5 line 22).

13. Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the information is collected by the firewalls automatically (Summary).

14. Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Conklin teaches wherein the information is transmitted utilizing an HTTP protocol (Summary and Column 7 lines 17 – 38).

15. Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the information is heuristically analyzed (Summary and Column 4 line 46 – Column 5 line 22).

16. Claim 12 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the identification of the source includes identifying an Internet Protocol (IP) address associated with at least one source of the intrusion activity (Summary; Column 3 lines 3 – 11 and Column 5 line 26 – Column 6 line 12).

17. Claim 14 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the notification includes an electronic mail (Summary and Column 7 line 17 – Column 8 line 13).

18. Claim 15 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches wherein the notification includes a summary of the intrusion activity (Summary and Column 5 lines 9 – 29).

19. Claim 16 is rejected as applied above in rejecting claim 10. Furthermore, Conklin teaches determining whether a response to the notification is received (Summary and Column 5 lines 9 – 29).

20. Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Conklin teaches wherein the response includes the rules (Summary and Column 4 line 45 – Column 5 line 22).

21. Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Conklin teaches wherein the information is collected by the firewalls periodically (Summary and Column 6 lines 47 – 63).

22. Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Conklin teaches wherein the identification of the source further includes looking up an electronic-mail address based on the IP address (Summary; Column 3 lines 3 – 11 and Column 5 line 26 – Column 6 line 12).

23. Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Conklin teaches wherein if it is determined that the response to the notification is not received, reporting the source of the intrusion activity to a central intrusion activity watch service (Summary and Column 8 lines 1 – 24).

24. Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Conklin teaches wherein the central intrusion activity watch service notifies the public of the source of the intrusion activity via a web interface (Summary and Column 7 lines 17 – 38).

Conclusion

25. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the

responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
October 01, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100